State of Montana

Commissioner of Political Practices

Agency IT Plan

Fiscal Year 2012-2017

May 2012

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Commissioner of Political Practices is a small, independent regulatory agency responsible for the collection of campaign finance information and lobbyist financial disclosure information. Currently, those responsibilities are met by offering both paper filing and online filing of those disclosure statements.

The 2007 legislature passed a law mandating electronic filing of disclosure reports for *statewide* candidates. As a result of this legislative mandate the agency adopted an administrative rule mandating *statewide* candidates use Campaign Tracker to submit their disclosure reports. Although, the office does have the capability for candidates and committees to file their disclosure statements online, the online environment is unstable due to several factors. First, the Access database was converted to an Oracle database in 2005. The database was architected to support storage of data but does not include accounting functionality. The online service and staff have had to develop multiple workarounds to accommodate the online filings. Other factors are the lack of appropriate funding, obsolescence and issues outside of agency control. In addition the agency has to contract for IT administration since the office has no IT FTE.

The agency is working closely with ITSD and vendors to develop both an adequate database and online interface that meets the needs of the candidates, committees, media, public and the agency. This initiative will require appropriate funding, a single vendor to handle both the front and back end development, and a professional IT administrator to oversee the project.

The online filing system is intended to eventually replace the current paper filing process. Additionally, the system would allow the public, media, and researchers to access all required financial disclosure statements for each of the required filers via a searchable web-based interface, replacing an inconvenient and burdensome source document search process.

SECTION 1: AGENCY ADMINISTRATIVE INFORMATION

Role: Plan Owner

Name:	James W. Murry
Telephone Number:	406-444-4622
Email Address:	jmurry@mt.gov

Role: IT Contact

Name:	Mary Baker
Telephone Number:	406-444-7416
Email Address:	mabaker@mt.gov

Role: IT Contact (Alternate)

Name:	Kym Trujillo
Telephone Number:	406-444-4627
Email Address:	ktrujillo@mt.gov

Role: Information Security Manager (ISM)

Name:	
Telephone Number:	
Email Address:	

IT Inventory

The IT inventory database located at http://mine.mt.gov/enterpriseitinventory was or will be updated on 6/25/12. As required by MCA 2-17-524(3)(c) the plan will be updated by June 30th, 2012.

SECTION 2: AGENCY IT MISSION

To provide Montana candidates, political committees, principals, and lobbyists the ability to register and file all required statements and reports via the Internet. To provide the citizens of Montana access to campaign finance and lobbying financial information via an Internet-ready database that provides complete and accurate data of all finances related to campaigns and lobbying activities in a timely manner and in a user friendly format.

SECTION 3: AGENCY REQUIRED PROGRAMS

Information Security Management (ISM) Program General Description

<The *department name* has implemented a department-wide (agency) information security management program compliant with §2-15-114, MCA and State Information Technology Systems Division *Information Security Programs* policy with adoption of the National Institute of Standards and Technology (NIST) Special Publication 800 series as guides for establishing appropriate security procedures. This is in alignment with the State of Information Technology Service's direction for an enterprise approach to protect sensitive and critical information being housed and shared on State and/or external/commercial information assets or systems.

As described in NIST SP 800-39, the agency has developed and adopted the Information Risk Management Strategy to guide the agency through information security lifecycle architecture with application of risk management. This structure provides a programmatic approach to reducing the level of risk to an acceptable level, while ensuring legal and regulatory mandates are met in accordance with MCA §2-15-114.

The agency's program has four components, which interact with each other in a continuous improvement cycle. They are as follows:

- Risk Frame – Establishes the context for making risk-based decisions
- Risk Assessment – Addresses how the agency will assess risk within the context of the risk frame; identifying threats, harm, impact, vulnerabilities and likelihood of occurrence
- Risk Response – Addresses how the agency responds to risk once the level of risk is determined based on the results of the risk assessment; e.g., avoid, mitigate, accept risk, share or transfer
- Risk Monitoring -- Addresses how the agency monitors risk over time; "Are we achieving desired outcomes?"

The agency's information security management program is challenged with limited resources; manpower and funding. While alternatives are reviewed and mitigation efforts are implemented the level of acceptable risk is constantly challenged by the ever changing technology and associated risks from growing attacks and social structure changes. Specific vulnerabilities have been identified which require restructure, new equipment, or personnel positions (funds increase), and are addressed below in our future plans. >

Future Security Program Plans

<Over this strategic period we plan to develop and implement ...>

Continuity of Operations (COOP) Capability Program General Description

<On *date* the *department name* joined with the Department of Administration *Continuity Services* for the development of our agency's Continuity of Operations Capabilities, which will provide the plans and structure to facilitate response and recovery capabilities to ensure the continued performance of the State Essential Functions of Government. This program involves two Blocks of focus; the first is to complete the Business Continuity Plans (BCP) involving two phases, the second Block works on the specific business processes or activity plans such as Emergency Action Plans (EAP), Information System Contingency Plan (ISCP), Communications Plans, Incident Management Plans, and more. We have completed ??? of 2 BCP phases and expect full completion of both Blocks by *date*. This program is not a standalone process in that information which is identified and recorded under this structure can and often exists in the Records Management Program and associates with Information Security Management Program requirements.

Integration of these three programs is critical to the confidentiality, integrity, and availability of information, which is associated with each program. >

Future COOP Program Plans

<Over this strategic period we plan to develop and implement

SECTION 4: AGENCY IT PLAN – GOALS & OBJECTIVES

Goal Number 1:

IT Goal 1 ~~Reduce the high risk of system failure due to outdated database functionality, fragile~~ online applications, and costly workarounds.

Rewrite the entire system using the lobbyist application as a prototype and Stoneriver as a single vendor. This would eliminate the possibility of losing functionality and gives the opportunity to eliminate the work arounds that have been developed over time to accommodate online filing. In addition the new database/web interface will alleviate the communication and fragile nature of these services since one vendor will have access and control of all of the moving parts of the applications.

Everyone benefits from this initiative; people running for elected office, political committees and the general public. The agency and State of Montana will also benefit because the risk of system failure will decrease significantly and the consistent costs for workarounds will be addressed during development therefore eliminating the constant need for change orders.

Reduces the risk of system failure. Provides quality online applications for customers and electronic access to disclosure data to the public.

Supporting Objective/Action

Objective 1-1 Engage a project management expert

The agency does not have a professional IT FTE. The agency will be dependent on a project manager to develop assessments, risks and alternatives throughout the development and implementation of this initiative.

The benefit of having a professional project manager is that the rewrite of the database and application is planned, organized, deliberate, and cost effective.

The project manager will be expected to prepare and deliver recommendations to the team, keep the team alerted of risks and contingencies, and ensure that deadlines or milestones are being met.

SECTION 5: IT INITIATIVES (FY2012 – FY 2017)

Initiative 1 Campaign Reporting Services/Database

The agency is working closely with ITSD and vendors to develop both an adequate database and online interface that meets the needs of the candidates, committees, media, public and the agency. This initiative will require appropriate funding, a single vendor to handle both the front and back end development, and a professional IT administrator to oversee the project.

EPP Number (if applicable) 32002

SECTION 6: ENTERPRISE ALIGNMENT

Communities of Interest Participation

- [x] Government Services
- [ ] Public Safety
- [ ] Human Resources
- [ ] Environmental
- [x] Education
- [x] Economic
- [ ] Cultural Affairs
- [x] Finance

SECTION 7: PLANNED AGENCY IT EXPENDITURES

Expense Category	FY2012	FY2013	FY2014	FY2015	FY2016	FY2017
Personal Services						
Operating Expenses						
Initiatives			$518,000			
Other expenditures						
Totals	0	0	$518,000	0	0	0

SECTION 8: ADDITIONAL INFORMATION - OPTIONAL

Attached is a Risk Assessment regarding our applications and an analysis completed by Dave Carlson at ITSD

State Information Technology Service Division (SITSD) Risk Assessment for Candidate Reporting Service Commissioner of Political Practices (CPP)

STEP 1: SYSTEM CHARACTERIZATION

Output from Step 1 - Characterization of the IT system being assessed, a good picture of the IT system environment, and delineation of the system boundary

The Candidate Registration and Reporting service is a web-based application that is integrated with two Oracle databases. One is built and maintained by Montana Interactive (MI) and stores all data prior to filing with the Commissioner of Political Practices; while the second is built and maintained by StoneRiver and hosted by SITSD. All systems and processes are managed by the Commissioner of Political Practices.

STEP 2: THREAT IDENTIFICATION

Output from Step 2 - A threat statement containing a list of threat-sources that could exploit system vulnerabilities

2.1 Threat Source Identification:

Candidates running for political office are required to register with the Commissioner of Political Practices and file campaign finance reports throughout the election cycle on a scheduled basis. Certain election cycles see more candidates than others with the most occurring during statewide elections; especially those that coincide with Presidential elections.

Candidates running for statewide office incur an extremely high number of contributions and expenditures which translates into significant amounts of data being reported within each campaign finance report. This information can be data entered individually or uploaded as bulk files directly into the Candidate Reporting service. Uploaded data is inserted into both the MI and CPP databases using stored procedures.

A routine practice of many political candidates is to wait until the last hour or often times the very last few minutes to file their campaign finance report. Given the sheer number of candidates and the potential amounts of data being reported, there is a risk of a tremendous load on the service in a very short amount of time which could potentially lead to failure.

2.2 Motivation and Threat Actions:

The Commissioner of Political Practices has indicated his intent to move forward with a mandate that will require all statewide candidates to file their campaign finance reports electronically. This will increase the number of customers utilizing the service as well as the amount of data being reported.

STEP 3: VULNERABILITY IDENTIFICATION

Output from Step 3 - A list of the system vulnerabilities that could be exercised by the potential threat-sources

Table 1- Potential Vulnerabilities Table

Vulnerability	Threat-Source	Threat-Action
A massive peak load	Users of the Service	In the case that this vulnerability occurred, the service would need to be restarted.

3.1 Vulnerability Sources:

The overall usage of the service to the point of load failure.

3.2 System Security Testing:

Stress testing information – the service has been load tested and has demonstrated its ability to handle the projected traffic over a period of a few hours, however, it cannot handle the traffic if most of the filings occur at the same time.

The most recent stress test load testing was conducted December 13-15, 2011. The load tests were based upon historical data from Commissioner of Political Practices.

Races	# Candidates	# Reports required	Contributions	Expenditures	Outstanding Debts	Corrections
Statewide	31	16	2183	93	0	0
State District	335	4	323	25	14	0
County	313	4				

A stress test was conducted as part of the load testing. This test was designed to simulate a massive peak load as if all state-wide candidates filed at the same time. The test included 40 statewide candidates all uploading 5000 Schedule A records, 500 Schedule B records and 25 Schedule C records at the same time.

The stress test was unsuccessful. The service experienced load failure and stopped functioning when all test users uploaded reports at the same time. All test users were unable to complete the upload process at the time the service stopped functioning. This was due not only to the volume of reports beign filed but also the number of records included in each filing.

STEP 4: CONTROL ANALYSIS

Output from Step 4 - List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event

4.1 Control Methods:

Various efforts will be pursued to attempt to lessen the possibility of a massive peak load on the Candidate Reporting service including:

- *Outreach* – the Commissioner of Political Practices will contact all candidates prior to and throughout each reporting deadline to encourage them to file their reports early and not wait until the last hour
- *Alter candidate reporting deadlines* – the Commissioner of Political Practices will pursue legislation to alter the reporting deadlines for the different candidate types to prevent all candidate types from having to file campaign finance reports on the same day. Statewide candidates still pose a significant challenge given the large amounts of data they have to report, however, eliminating all other candidate types should help minimize the load on the service.
- *Limit related service availability* – as soon as campaign finance reports are filed they can be viewed through the Candidate Search and Download service. The immediacy of the report availability is often the reason for delayed filing. The Commissioner of Political Practices intends to limit the availability of the Search and Download site on reporting deadline days in the hopes that this will make candidates more comfortable with filing earlier in the day.

STEP 5: LIKELIHOOD DETERMINATION

Output from Step 5 - Likelihood rating (High, Medium, Low)

Table 2 - Likelihood Definitions

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

The likelihood of a massive peak load vulnerability occurring is high.

STEP 6: IMPACT ANALYSIS

Output from Step 6 - Magnitude of Impact (High, Medium, or Low)

Table 3 - Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

The impact of a massive peak load vulnerability occurrence is high.

STEP 7: RISK DETERMINATION

Output from Step 7 - Risk level (High, Medium, Low)

7.1 Risk Level Matrix:

The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low.

The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

Table 4 - Risk-Level Matrix

Threat Likelihood	Impact: Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)***

****If the level indicated on certain items is so low as to be deemed to be "negligible" or non significant (value is 1 on risk scale of 1 to 100), one may wish to hold these aside in a separate bucket in lieu of forwarding for management action. This will make sure that they are not overlooked when conducting the next periodic risk assessment. It also establishes a complete record of all risks identified in the analysis. These risks may move to a new risk level on a reassessment due to a change in threat likelihood and/or impact and that is why it is critical that their identification not be lost in the exercise.****

The risk level for a massive peak load vulnerability is 100, or high.

7.2 Description of Risk Level:

Table 5 - Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

The Commissioner of Political Practices is aware of the risk rating and accepts the risks associated with the massive peak load vulnerability.

STEP 8: CONTROL RECOMMENDATIONS

Output from Step 8 - Recommendation of control(s) and alternative solutions to mitigate potential risk

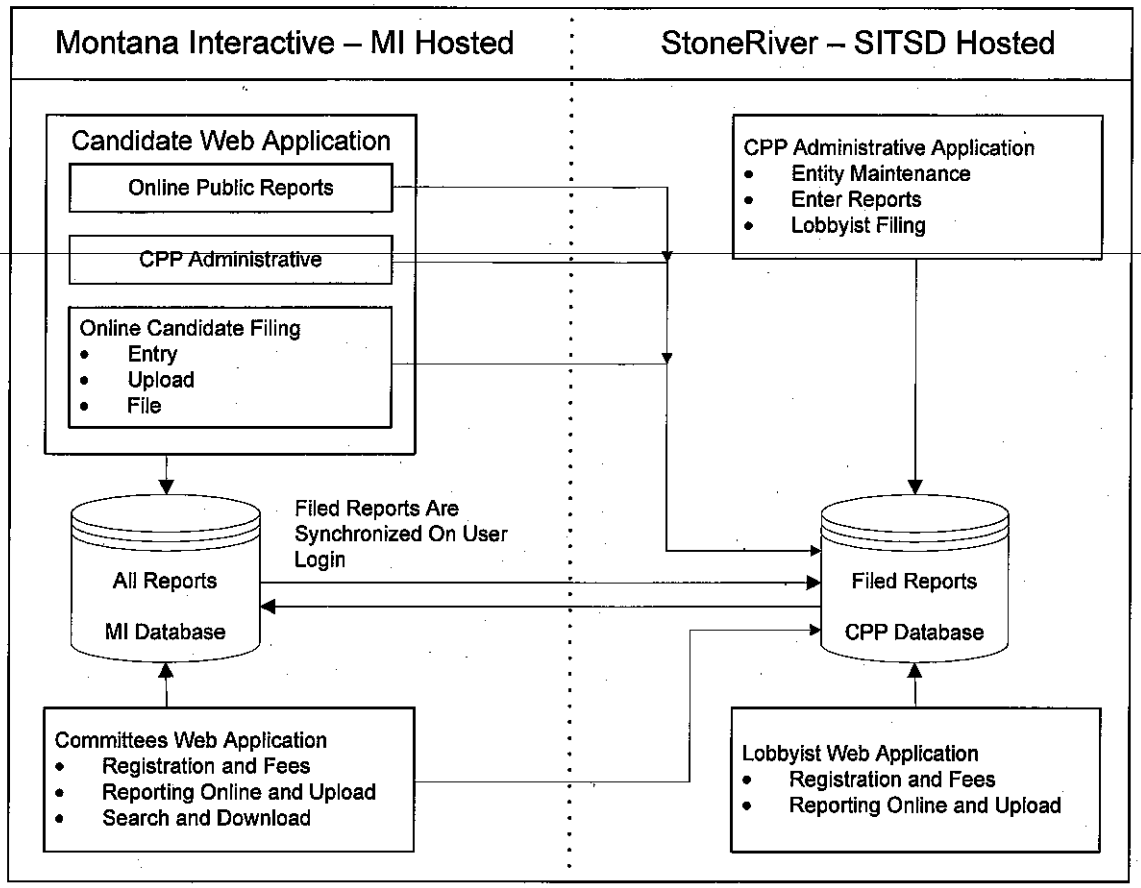
The most significant liability in connection with a system failure due to a massive peak load vulnerability is the negative portrayal of a system failure by the media and the customers of the services, which are candidates running for elected offices. The risk mitigation plan detailed in steps 4 and 8, in part, includes that all parties involved in connection with the service provide a consistent message in the case of a system failure.

It is important that all parties involved, the Commissioner of Political Practices, SITSD and MI, are in agreement regarding communicating about the service. This is especially true in the case of a system failure. As owners of the service, the Commissioner of Political Practices will serve as the single point of contact, in connection with inquires from the press and/or candidates running for elected office regarding the service. The parties to the agreement will convey a positive, unified message on behalf of all parties. The parties to the agreement will not segregate any individual party, such as CPP, SITSD or MI, when publicly discussing any potential negative issues that may arise concerning the service.

If any of the parties in connection with the service become aware of a problem with service they will promptly notify MI and give MI the opportunity to investigate the problem before any additional information is provided to a third party.

Jim Murry Commissioner of Political Practices	Date
Sandi Miller, General Manager Montana Interactive, LLC	Date
Audrey Hinman, Chief Architecture and Internet Services Bureau Information Technology Services Division Department of Administration	Date

Campaign Tracker Candidate Service Analysis – 4/18/2012



Issues/Concerns/Etc.

- CPP staff files for candidates using the MI online filing tool
- The CPP database was designed to accomplish a specific goal 8 years ago and is not able to accommodate the current functionality demands
- The MI web application is very complex and fragile as a result of workarounds created to accommodate the inadequacies of the CPP database
- The CPP Administrative Application lacks functionality that is required for the CPP's current business processes
- Three separate applications maintained by two different vendors are connected to the same database
- Frequent change of vision as a result of frequent changes in leadership
- Small non-technical staff at CPP
- No accounting functionality in CPP database
- Data modified to display correctly in one application displays incorrectly in the other application
- Data discrepancies in reports as a result of workarounds/differences between the MI and CPP databases
- CPP business processes have been adapted to accommodate the applications which involves a lot of manual work on the part of the staff
- Lobbyist application works well and could be the prototype for a rewrite of the rest of the system
- Difficult to uniquely identify contributors which leads to frequent duplicate entries

Options

- COTS or SAS product – Projected Cost $1m+
- Rewrite entire system using Lobbyist application as prototype and StoneRiver as single vendor for CPP – Projected Cost $400k – Could be completed in 6 months for existing functionality only
- Rewrite part of the system – CPP is currently considering rewriting the Administrative Application and redesigning the CPP database – Projected Cost $200k